УДК 004.021

ПРИМЕНЕНИЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА ДЛЯ ВЫЯВЛЕНИЯ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Перфильев В.Э., Акимов К.О., Тимофеев Р.С., Данзырын Б.Э. (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Научный руководитель – к.т.н., доцент Менщиков А.А.

(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Данная работа посвящена применению генетического алгоритма в системе дистанционного банковского обслуживания с целью выявления мошеннических транзакций. Генетический алгоритм выявления мошеннических транзакций основан на анализе конечного набора шаблонов поведения.

Введение. Экспертные системы, основанные на правилах, были успешно реализованы для широкого спектра бизнес-приложений, включая страхование, обнаружение мошенничества, настройку компонентов, регулирование процессов, интеллектуальное обучение, медицинскую диагностику, проектирование схем и многих других. Ключевой трудностью при разработке этих систем является получение оценки экспертных знаний и её автоматизация для каждого случая, например финансового мошенничества, что все еще является серьезной проблемой для банковских организаций. В связи с этим применение экспертных систем в обнаружении мошеннических транзакций и графовое представление структуры данных для классификации на предмет мошеннических операций формируют цели данного исследования в области кибербезопасности банковской сферы.

Основная часть. Использование графов для представления базы данных транзакций банковской сети позволяет сформировать контейнер операций финансовой организации, для которой открывается широкий набор инструментов из теории графов. С помощью полученных инструментов можно качественно и быстро формировать вердикты для аномальных (мошеннических) транзакций. Для 2-го этапа исследования набор обрабатываемых операций ограничен лишь переводами денежных средств от одного пользователя к другому. В рамках данного исследования в качестве одного из источников данных по транзакциям, в том числе мошенническим, используется криптовалютная сеть Ethereum. Несмотря на принципиальные различия в подходах создания и использования финансовой сети внутри банковской организации и криптовалютах, опыт работы с децентрализованными сетями можно применить для централизованной сети. Для представленной графовой структуры с помощью конечного набора правил выбора источника данных и самих данных был сформировать конечный набор эталонных значений предикторов, отклонение от которых является признаком мошеннической активности. Таким образом, было выделено 3 слоя для системы обнаружения мошенничества:

1) множество шаблонов выбора источника данных;
2) множество шаблонов выбора набора данных из полученного с предыдущего слоя источника;
3) множество шаблонов способов сравнения набора данных с предыдущего слоя с эталонными значениями;

Необходимо было из всего множества правил выделить такое сочетание правил, комбинация которых с наибольшей вероятностью соответствует мошенническому поведению и может называться системой правил определения мошеннической активности. Размерность задачи кратно (степенная зависимость) возрастает с увеличением количества шаблонов. Таким образом использование генетического алгоритма для решения оптимизационной задачи

(поиск максимума). В качестве ядра генетического алгоритма предлагается использовать видоизмененную библиотеку pyeasyga.

Выводы. Представлено общее описание алгоритма противодействия осуществлению переводов денежных средств без согласия клиента, в том числе выявление мошеннических операций в системах ДБО на основе анализа графов с помощью генетического алгоритма.

Список использованных источников:

1. Improving a Rule-based Fraud Detection System with Classification Based on Association Rule Mining [Электронный ресурс] // Michaela Baumann // NÜRNBERGER Versicherung – Режим доступа: https://www.researchgate.net/publication/358414759_Improving_a_Rule-based_Fraud_Detection_System_with_Classification_Based_on_Association_Rule_Mining (дата обращения 10.01.2023);
2. InfDetect: a Large Scale Graph-based Fraud Detection System for E-Commerce Insurance [Электронный ресурс] // Cen Chen, Chen Liang, Jianbin Lin, Li Wang, Ziqi Liu, Xinxing Yang, Jun Zhou, Yang Shuang, Yuan Qi // AI Department, Ant Financial Services Group – Режим доступа: https://ieeexplore.ieee.org/abstract/document/9006115 (дата обращения: 11.01.2023);
3. A semantic rule based digital fraud detection [Электронный ресурс] // Mansoor Ahmed, Kainat Ansar, Cal B. Muckley, Abid Khan, Adeel Anjum1, Muhammad Talha // Department of Computer Science, COMSATS University Islamabad; Innovation Value Institute, Maynooth University, Maynooth; UCD College of Business and Geary Institute, Dublin; Department of Computer Science, Aberystwyth University, Aberystwyth – Режим доступа: https://www.researchgate.net/publication/353704173_A_semantic_rule_based_digital_fraud_detection (дата обращения: 21.01.2023);
4. Remi-Omosowon A., Gonzalez Y. Библиотека pyeasyga [Электронный ресурс] // Режим доступа: https://pyeasyga.readthedocs.io/en/latest/usage.html (дата обращение: 13.02.2023).

Перфильев В.Э. (автор)	Подпись
Акимов К.О. (автор)	Подпись
Тимофеев Р.С. (автор)	Подпись
Данзырын Б.Э. (автор)	Подпись
Менщиков А.А. (научный руководитель)	Подпись